

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

_____ Євген СОКОЛ

«___» _____ 2026 р.

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»**

Першого (бакалаврського) рівня вищої освіти

за спеціальністю **F5 – Кібербезпека та захист інформації**

галузі знань **F – Інформаційні технології**

кваліфікація **бакалавр з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова вченої ради

_____ / Євген СОКОЛ

Протокол № _____

від «___» _____ 2026 р.

Харків 2026 р.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми «Кібербезпека»

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	F – Інформаційні технології
Спеціальність	F5 – Кібербезпека та захист інформації
Кваліфікація	Бакалавр з кібербезпеки та захисту інформації

СХВАЛЕНО

Робочою групою ОПП із спеціальності
«Кібербезпека та захист інформації»

Гарант ОПП

_____ Сергій ЄВСЕЄВ

Протокол №__

«__» _____ 2026 р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

_____ Руслан МИГУЩЕНКО

Протокол №__

«__» _____ 2026 р.

ПОГОДЖЕНО

Завідувач кафедри
кібербезпеки

_____ Сергій ЄВСЕЄВ

Протокол №__

«__» _____ 2026 р.

ПОГОДЖЕНО

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних
технологій

_____ Михайло ГОДЛЕВСЬКИЙ

«__» _____ 2026 р.

ПОГОДЖЕНО

Здобувач вищої освіти
(член робочої групи ОПП)
№ групи КН-11226

_____ Діана СПІКО

«__» _____ 2026 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ

Наказом ректора Національного технічного університету «Харківський політехнічний інститут» від «__» _____ 2026 року № ____.

Ця освітньо-професійна програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Національного технічного університету «Харківський політехнічний інститут».

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-професійної програми одержано від:

1. Іван ОПРСЬКИЙ, доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»
2. Владислав КОВТУН, кандидат технічних наук, доцент, директор ТОВ «Сайфер»
3. Сергій ГОЛОВАШИЧ, кандидат технічних наук, доцент директор ТОВ «Мікрокрипт Текнолоджіс»
4. Олена ВОЛОЩУК, кандидат технічних наук, керівник освітніх програм ТОВ «Distributed Lab».
5. Ольга ШАПОВАЛ, виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»

Рецензії

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти першого (бакалаврського) рівня галузі знань F “Інформаційні технології”, спеціальності F5 “Кібербезпека та захист інформації”, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547.

Розроблено робочою групою освітньо-професійної програми “Кібербезпека” Навчально-наукового інституту комп’ютерних наук та інформаційних технологій Національного технічного університету “Харківський політехнічний інститут” у складі:

Гарант освітньо-професійної програми

Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.

Члени робочої групи ОПП:

1. Ольга КОРОЛЬ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.
2. Сергій ПОГАСІЙ, доктор технічних наук, доцент, професор кафедри кібербезпеки.
3. Станіслав МІЛЕВСЬКИЙ, доктор технічних наук, доцент, професор кафедри кібербезпеки.
4. Діана СПІКО, студентка групи КН-11226.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ F5 – КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет “Харківський політехнічний інститут”, Навчально-науковий інститут <u>комп’ютерних наук та інформаційних технологій</u> кафедра <u>кібербезпеки</u>
Ступінь вищої освіти та назва кваліфікації (освітньої, професійної) мовою оригіналу	Бакалавр Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації. Кваліфікація в дипломі: бакалавр з кібербезпеки та захисту інформації.
Професійна кваліфікація	Відсутня
Форма навчання	Інституційна (очна (денна)), заочна.
Офіційна назва освітньої програми	Кібербезпека
Назви спеціалізацій (предметних спеціальностей)	Відсутня
Тип диплому одиничний, спільний (подвійний) за наявності та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Сертифікат про акредитацію освітньої програми № 9111. Термін дії – 01.07.2029р.
Цикл/рівень	Перший (бакалаврський) рівень вищої освіти; НРК України – 6 рівень; EQF LLL – 6 рівень; FQ-EHEA – перший цикл.
Передумови	Для здобуття освітнього ступеня бакалавра зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту. Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством.
Мова викладання	Українська мова, Англійська мова
Термін дії освітньо-професійної програми	Відповідно до терміну дії сертифікату Переглядається щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-bakalavr/

2 – Мета освітньо-професійної програми	
Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність, спеціалізація або предметна спеціальність (за наявності))	Галузь знань: F “Інформаційні технології” Спеціальність: F5 “Кібербезпека та захист інформації” Об’єкти вивчення: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; – безпека інформаційних ресурсів, систем та технологій, штучного інтелекту, об’єктів інформаційної діяльності та критичної інфраструктури. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області: теорії, поняття, концепції, принципи захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, безпеки інформаційних систем та технологій, забезпечення своєчасного виявлення, запобігання і нейтралізації цільових (змішаних) атак, об’єктів інформаційної діяльності та критичної інфраструктури у кіберпросторі. Методи, методики та технології: методи, методики та технології, дослідження, моделювання, аналізу та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів, розв’язання теоретичних і практичних задач кібербезпеки та захисту інформації у кіберпросторі, виявлення, аналізу кіберінцидентів і протидії ним, запобігання і нейтралізації реальних і потенційних загроз інформаційним ресурсам, об’єктам інформаційної діяльності та критичної інфраструктури, створення, супроводження та забезпечення ефективного функціонування систем захисту інформації, дослідження та вдосконалення процесів обробки та захисту інформаційних ресурсів. Інструменти та обладнання: прикладне та спеціалізоване програмне забезпечення, мережне устаткування, апаратне забезпечення, засоби та пристрої захисту інформації.
Орієнтація освітньої програми	Освітньо-професійна. Підготовка фахівців у сфері кібербезпеки та захисту інформації.
Основний фокус освітньої програми та спеціалізації або предметна спеціальність (за наявності)	Спеціальна освіта у галузі інформаційних технологій зі спеціальності F5 “Кібербезпека та захист інформації”. Поглиблене вивчення інформаційних технологій захисту інформації, інформаційної безпеки, кібербезпеки, та безпеки інформації, розробки та використання програмного забезпечення захисту інформації, кібербезпеки та інформаційної безпеки.

	Ключові слова: кібербезпека, інформаційна безпека, захист інформації, інформаційні технології.
Особливості програми	Особливістю програми спеціальності “Кібербезпека та захист інформації” є орієнтація на сучасні вимоги до фахівців в галузі інформаційної та/або кібербезпеки, набуття здобувачами вищої освіти конкурентоспроможних компетентностей на основі синергізму отримання результатів навчання з інформаційної та/або кібербезпеки та програмування, використання курсів мережевої академії Cisco з Networking, Cybersecurity, IoT & Data Analytics, OS and IT, Programming Courses. Можливість навчатися англійською мовою.
4 – Придатність випускників до працевлаштування та академічні права випускників	
Придатність до працевлаштування	Працевлаштування на посади у структурних установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації. Фахівці з кібербезпеки та захисту інформації можуть працювати на посадах, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010, а саме: 2139.2 Фахівець сфери захисту інформації; 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології); 2139.2 Фахівець з підтримки інфраструктури кіберзахисту; 2139.2 Фахівець з реагування на інциденти кібербезпеки; 2139.2 Фахівець з криптографічного захисту інформації; 2139.2 Фахівець з технічного захисту інформації; 2139.2 Фахівець з тестування систем безпеки та захисту інформації; 2139.2 Аудитор інформаційних технологій (з кібербезпеки); 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки).
Академічні права випускників	Здобувачі освіти, які пройшли підготовку за даною навчальною програмою та отримали диплом бакалавра, мають право на здобуття освіти на другому (магістерському) рівні вищої освіти у ЗВО України та за кордоном в галузі знань “Інформаційні технології” або суміжних. Здобуття або вдосконалення освіти та професійної підготовки в системі дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, проблемно-орієнтоване навчання, дистанційне навчання в системі Microsoft 365, самонавчання, навчання через проєктну практику, навчання через лабораторну практику. У процесі викладання передбачено застосування таких навчальних технологій, як: лекції, лабораторні роботи, практичні заняття, робота в малих групах, семінари-дискусії, brainstorming, презентації, що розвивають комунікативні та лідерські навички, самостійна

	робота з літературними джерелами; змішані форми навчання з використанням дистанційних платформ.
Оцінювання	Моніторинг знань та умінь студентів здійснюється у формі поточного та підсумкового контролю. Поточний контроль – усне та письмове опитування, оцінка роботи в малих групах, тестування, захист групових та індивідуальних науково-дослідних завдань. Підсумковий контроль – усні та письмові екзамени, заліки з урахуванням накопичених балів поточного контролю, захист звітів з лабораторних занять, захист курсових робіт. Державна атестація – єдиний державний кваліфікаційний іспит. Оцінювання здійснюється за національною шкалою (“відмінно”, “добре”, “задовільно”, “незадовільно”), 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (визначені стандартом вищої освіти спеціальності)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові) компетентності (визначені стандартом вищої освіти спеціальності)	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту

	інформації. СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 – Результати навчання	
Результати навчання за спеціальністю (визначені стандартом вищої освіти спеціальності)	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН7. Застосовувати й адаптувати теорії інформації та

	кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах
--	---

	інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України “Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти” від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 15-16). Склад робочої групи освітньої програми, професорсько викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти. До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також закордонні фахівці.
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України “Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти” від 30 грудня 2015 р., № 1187, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 17). Навчально-науково-виробнича база у вигляді: –навчальні корпуси, комп'ютерні класи, об'єднані локальною обчислювальною мережею з виходом до Інтернету, мультимедійне обладнання;–спеціалізоване програмне забезпечення, кіберполігон.
Інформаційне та навчально-методичне забезпечення	Відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України “Про

	затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти” від 30 грудня 2015 р., № 1187, (зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 18). Інформаційне та навчально-методичне забезпечення навчального процесу реалізується наявністю необхідної навчальної та методичної літератури: підручники, навчальні посібники, методичні рекомендації до практичних занять, самостійної роботи, силабуси освітніх компонентів (https://cybersecurity.khpi.edu.ua/sylabusy-osvitnikh-komponentiv-f5-bakalavr/). Інформаційні ресурси розміщені у фондах наукової бібліотеки НТУ “ХПІ”, сайтах випускових кафедр. У навчальному процесі застосовується LMS (Learning Management System).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів про академічну мобільність з університетами України. Угоди про співпрацю щодо реалізації програм внутрішньої академічної мобільності здобувачів вищої освіти за освітньою програмою “Кібербезпека” спеціальності F5 “Кібербезпека та захист інформації” з Одеським національним технологічним університетом, Чернігівським національним технологічним університетом.
Міжнародна кредитна мобільність	На основі двостороннього договору з університетом ім. Яна Длугоша в м. Ченстохові (Польща).
Навчання іноземних здобувачів вищої освіти	Підготовка іноземних громадян здійснюється згідно з вимогами чинного законодавства за умови визнання попереднього освітнього рівня.

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент освітньо-професійної програми

Код о/к	Компоненти освітньої програми (дисципліни, проекти / роботи, практика, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові освітні компоненти ОПП			
1.1 Загальна підготовка			
ЗП 1	Історія української державності	4,0	Екзамен
ЗП 2	Українська мова (професійного спрямування)	3,0	Залік
ЗП 3	Іноземна мова	16,0	Залік, Екзамен
ЗП 4	Фізика	4,0	Екзамен
ЗП 5	Основи гуманітарно-філософських знань у професійній діяльності	4,0	Екзамен
ЗП 6	Вища математика	6,0	Залік
ЗП 7	Основи вищої алгебри	5,0	Екзамен
ЗП	Фізичне виховання	4,0	Залік
1.2 Спеціальна (фахова) підготовка			
СП 1	Вступ до спеціальності. Ознайомча практика	3,0	Залік
СП 2	Основи програмування	4,0	Екзамен
СП 3	Теорія інформації і кодування	5,0	Екзамен
СП 4	Правове регулювання захисту інформації	4,0	Залік
СП 5	Алгоритми та структури даних	5,0	Екзамен
СП 6	Фізичні основи технічних засобів розвідки	5,0	Екзамен
СП 7	Інформаційна безпека держави	4,0	Залік
СП 8	Методи соціальної інженерії в кібербезпеці	4,0	Залік
СП 9	Математичні основи криптології	4,0	Екзамен
СП 10	Технології програмування	5,0	Екзамен
СП 11	Комп'ютерні мережі	4,0	Екзамен
СП 12	Захист сучасних операційних систем	6,0	Залік
СП 13	Розробка програмного забезпечення систем кібербезпеки	6,0	Екзамен
СП 14	Основи криптографічного захисту	6,0	Залік
СП 15	Основи захисту мікропроцесорних систем	4,0	Екзамен
СП 16	Математичне моделювання систем безпеки	4,0	Екзамен
СП 17	Основи стеганографічного захисту інформації	5,0	Залік
СП 18	Безпека DevOps	4,0	Залік
СП 19	Розробка веб-додатків	6,0	Екзамен
СП 20	Комплексні системи захисту інформації	4,0	Екзамен
СП 21	Безпека інтернет-речей	4,0	Залік

СП 22	Веб-безпека	5,0	Залік
СП 23	Комплексний тренінг	4,0	Залік
СП 24	Нейронні мережі	5,0	Залік
СП 25	OSINT-розвідка	4,0	Залік
2. Практична підготовка			
ПП 1	Виробнича практика	6,0	Залік
ПП 2	Технологічна практика	6,0	Залік
3. Атестація			
	Атестація	3,0	
Загальний обсяг обов'язкових компонент		175	
4. Вибіркові освітні компоненти			
4.1 Профільна підготовка			
4.1.1 Профільований пакет освітніх компонент 01 “Штучний інтелект в системах захисту”			
ВП1.1	Етичний хакінг	3,0	Екзамен
ВП1.2	Дата майнинг	3,0	Екзамен
ВП1.3	Математичні основи штучного інтелекту	3,0	Екзамен
ВП1.4	Python для штучного інтелекту та машинного навчання	4,0	Екзамен
ВП1.5	Генетичні алгоритми	3,0	Екзамен
ВП1.6	Python для інтернет-речей	3,0	Екзамен
ВП1.7	Системний інжиніринг	3,0	Екзамен
4.1.2 Профільований пакет освітніх компонент 02 “Блокчейн-технологія та безпека банківських систем”			
ВП2.1	Децентралізовані системи	3,0	Екзамен
ВП2.2	Ризик-менеджмент	3,0	Екзамен
ВП2.3	Blockchain: основи та приклади застосування	3,0	Екзамен
ВП2.4	Безпека банківських систем	4,0	Екзамен
ВП2.5	Захист об'єктів критичної інфраструктури	3,0	Екзамен
ВП2.6	Організація документообігу з обмеженим доступом	3,0	Екзамен
ВП2.7	Безпека в соціальних мережах	3,0	Екзамен
4.1.3. Профільований пакет освітніх компонент 03 "Innovation Campus"			
ВП3.1	Основи кібербезпеки	3,0	Екзамен
ВП3.2	Розробка корпоративних інформаційних систем (частина 1)	3,0	Екзамен
ВП3.3	Розробка корпоративних інформаційних систем (частина 2)	3,0	Екзамен
ВП3.4	Бази даних для корпоративних інформаційних систем	4,0	Екзамен
ВП3.5	Архітектура корпоративних інформаційних систем	3,0	Екзамен
ВП3.6	Безпека та аудит бездротових та рухомих мереж	3,0	Екзамен
ВП3.7	Захист об'єктів критичної	3,0	Екзамен

	інфраструктури		
4.2. Освітні компоненти вільного вибору професійної підготовки загальноінститутського каталогу			
ОКВП 1	ОК ВВ ПК 1	4,0	Залік
ОКВП 2	ОК ВВ ПК 2	4,0	Залік
ОКВП 3	ОК ВВ ПК 3	4,0	Залік
ОКВП 4	ОК ВВ ПК 4	4,0	Залік
ОКВП 5	ОК ВВ ПК 5	4,0	Залік
ОКВП 6	ОК ВВ ПК 6	4,0	Залік
ОКВП 7	ОК ВВ ПК 7	4,0	Залік
4.3. Освітні компоненти вільного вибору загальноуніверситетського каталогу			
ОКВЗ 1	ОК ВВ ЗК 1	4,0	Залік
ОКВЗ 2	ОК ВВ ЗК 2	4,0	Залік
ОКВЗ 3	ОК ВВ ЗК 3	4,0	Залік
4.4. Освітні компоненти спеціального вибору університету			
ОКСВУ	ОК СВУ	3,0	Залік
Загальний обсяг вибірових компонент:		65	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		240	

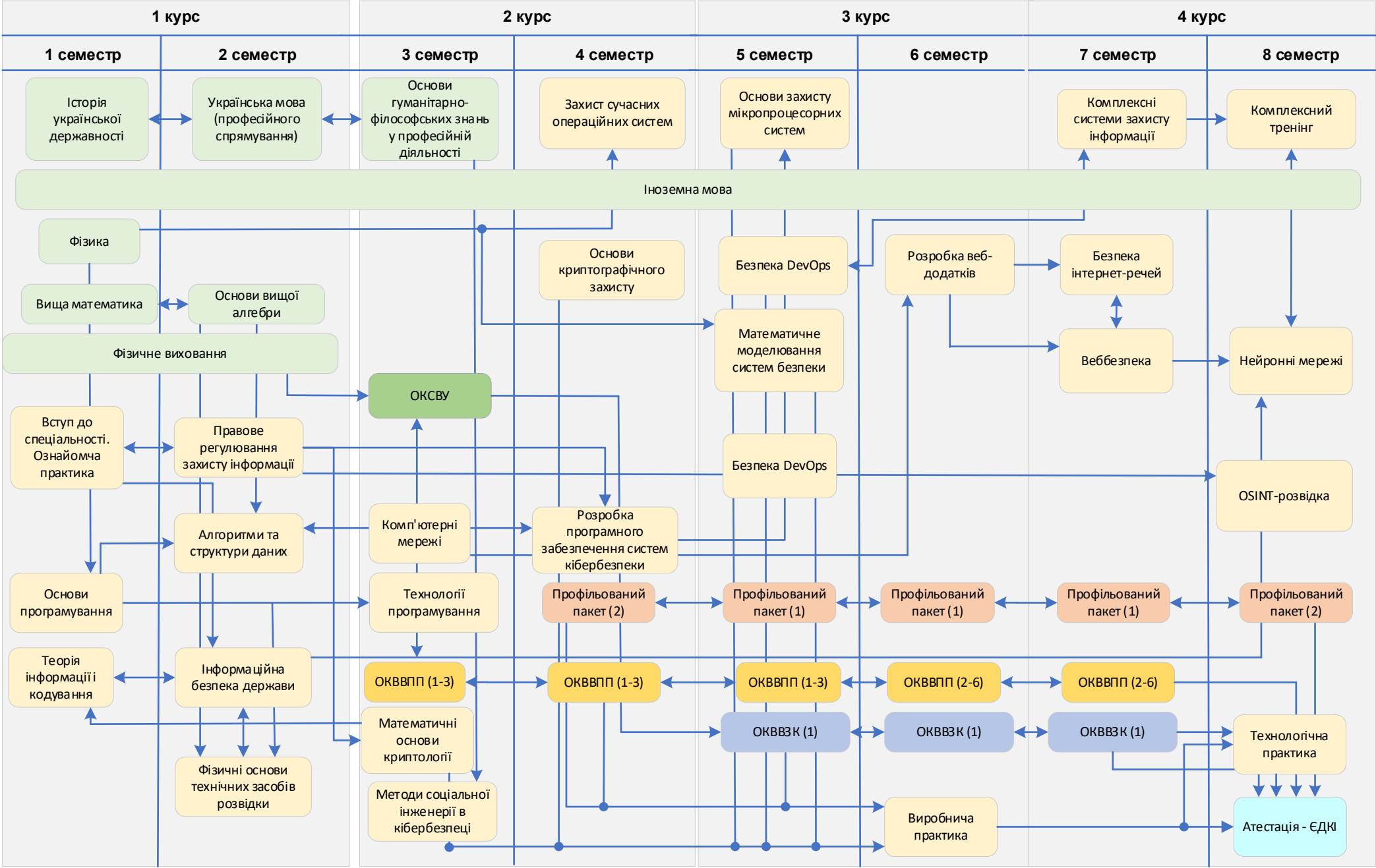
3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	46 / 19,2	-	46 / 19,2
2	Спеціальна (фахова) підготовка	114/ 47,5	-	114/ 47,5
3	Практична підготовка	12/5	-	12/5
4	Вибіркові освітні компоненти	-	65 / 27,1	65 / 27,1
5	Атестація	3/1,2	-	3/1,2
Всього за весь термін навчання		175 / 72,9	65 / 27,1	240 / 100

4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти спеціальності «Кібербезпека та захист інформації» та освітньою програмою.

5. СТРУКТУРНО-ЛОГІЧНА СХЕМА



6. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ СТАНДАРТОМ КОМПЕТЕНТНОСТЕЙ / РЕЗУЛЬТАТІВ НАВЧАННЯ ДЕСКРИПТОРАМ НРК

Класифікація компетентностей (результатів навчання) за НРК	Знання Зн1. Концептуальні наукові та практичні знання. Зн2. Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	Уміння Ум1. Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання.	Комунікація К1. Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень власного досвіду та аргументації. К2. Збір, інтерпретація та застосування даних. К3. Спілкування з професійних питань, у тому числі іноземною мовою	Відповідальність і автономія АВ1. Управління складною технічною або професійною діяльністю чи проектами. АВ2. Спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах. АВ3. Формування суджень, що враховують соціальні, наукові та етичні аспекти. АВ4. Організація та керівництво професійним розвитком осіб та груп. АВ5. Здатність продовжувати навчання із значним ступенем автономії.
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК1	Зн2	Ум1		
ЗК2	Зн2	Ум1	К1	
ЗК3			К1, К3	
ЗК4			К1, К3	
ЗК5	Зн1, Зн2	Ум1	К2	АВ3
ЗК6	Зн1		К1	АВ2, АВ3, АВ4
ЗК7			К1	АВ2
ЗК8	Зн2		К2	АВ3
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
СК1	Зн2	Ум1	К2	
СК2	Зн1, Зн2	Ум1	К2	
СК3		Ум1		АВ1
СК4		Ум1		АВ1
СК5		Ум1	К2	АВ1, АВ2
СК6		Ум1	К1	АВ1
СК7		Ум1	К1	АВ1
СК8	Зн2	Ум1		
СК9	Зн2	Ум1		
СК10		Ум1	К2	АВ2

[illegible]

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH2	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17				ЗП3 СП7 СП8 СП11 СП12 СП14 СП24														

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
РН3	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13						ЗП1 СП1 СП4 СП7	ЗП3 СП4 СП7											

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
РН4	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП21	ЗП4 ЗП СП2 СП3 СП4 СП5 СП7 СП8 СП9 СП10 СП11 СП12 СП14 СП15 СП16 СП19 СП21	ЗП4 ЗП5 ЗП6 ЗП7 СП1 СП2 СП4 СП5 СП6 СП7 СП10 СП13 СП14 СП15 СП16 СП17 СП18																

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2	СП22 СП23 СП24 СП25 ПП1 ПП2	СП19 СП20 СП21 СП22 СП23 СП25 ПП1 ПП2																
PH5	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5	ЗП4 ЗП СП2 СП3 СП4 СП5 СП7 СП8 СП9 СП10 СП11 СП12 СП14	ЗП4 ЗП5 ЗП6 ЗП7 СП1 СП2 СП4 СП5 СП6 СП7 СП10 СП13 СП14																

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2	СП15 СП16 СП19 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2	СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП25 ПП1 ПП2																
PH6	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1		ЗП4 ЗП5 ЗП6 ЗП7 СП1 СП2 СП4 СП5 СП6						ЗП1 ЗП4 ЗП5 ЗП СП1 СП3 СП17 СП20 СП23										

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2		СП7 СП10 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП25 ПП1 ПП2						СП25										
PH7	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5	ЗП4 ЗП СП2 СП3 СП4							ЗП1 ЗП4 ЗП5 ЗП СП1										

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2	СП5 СП7 СП8 СП9 СП10 СП11 СП12 СП14 СП15 СП16 СП19 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2						СП3 СП17 СП20 СП23 СП25											
PH8	ЗП1					ЗП4													

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24					ЗП6 ЗП7 СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП9 СП10 СП11 СП12 СП14 СП15 СП16 СП23 СП25													

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП25 ПП1 ПП2																		
РН9	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20						ЗП1 СП1 СП4 СП7			СП1 СП4 СП7 СП8 СП10 СП11 СП14 СП20 СП23 СП24									

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH10	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16									СП2 СП3 СП5 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1									

Результати навчання	Інтегральна компетентність	Компетентності																	
		Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH11	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12											СП11 СП14 СП20 СП21 СП24							

Результати навчання	Інтегральна компетентність	Компетентності																	
		Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH12	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8												СП9 СП11 СП12 СП14 СП19 СП20 СП21 СП22 СП23 СП24 СП25						

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH13	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4												СП9 СП11 СП12 СП14 СП19 СП20 СП21 СП22 СП23 СП24 СП25						

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH14	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП													СП8 СП11 СП14 СП15 СП21 СП24 СП25					

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП1																		
	СП2																		
	СП3																		
	СП4																		
	СП5																		
	СП6																		
	СП7																		
	СП8																		
	СП9																		
	СП10																		
	СП11																		
	СП12																		
	СП13																		
	СП14																		
	СП15																		
	СП16																		
	СП17																		
	СП18																		
	СП19																		
	СП20																		
	СП21																		
	СП22																		
	СП23																		
	СП24																		
	СП25																		
	ПП1																		
	ПП2																		
PH15	ЗП1													СП8					
	ЗП2													СП11					
	ЗП3													СП14					
	ЗП4													СП15					

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2													СП21 СП24 СП25						

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
PH16	ЗП1														СП11				
	ЗП2														СП12				
	ЗП3														СП14				
	ЗП4														СП20				
	ЗП5														СП23				
	ЗП6														СП25				
	ЗП7														ПП2				
	ЗП																		
	СП1																		
	СП2																		
	СП3																		
	СП4																		
	СП5																		
	СП6																		
	СП7																		
	СП8																		
	СП9																		
	СП10																		
	СП11																		
	СП12																		
	СП13																		
	СП14																		
	СП15																		
	СП16																		
СП17																			
СП18																			
СП19																			
СП20																			
СП21																			
СП22																			
СП23																			

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП24 СП25 ПП1 ПП2																		
PH17	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19														СП7 СП16 СП23 СП25 ПП1 ПП2				

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH18	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15																СП3 СП9 СП11 СП12 СП14 СП15 СП18 СП21 СП23 СП24 ПП2		

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH19	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11															СП3 СП9 СП11 СП12 СП14 СП15 СП18 СП21 СП23 СП24 ПП2			

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП12																		
	СП13																		
	СП14																		
	СП15																		
	СП16																		
	СП17																		
	СП18																		
	СП19																		
	СП20																		
	СП21																		
	СП22																		
	СП23																		
	СП24																		
	СП25																		
	ПП1																		
	ПП2																		
	PH20	ЗП1																	СП6
ЗП2																		СП12	
ЗП3																		СП14	
ЗП4																		СП15	
ЗП5																		СП19	
ЗП6																		СП20	
ЗП7																		СП22	
ЗП																		СП23	
СП1																		ПП2	
СП2																			
СП3																			
СП4																			
СП5																			
СП6																			
СП7																			

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		
PH21	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 ЗП6 ЗП7 ЗП СП1 СП2 СП3																		СП8 СП11 СП14 СП16 СП18 СП23 СП24 СП25 ПП1

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
	СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2																		

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Зауваження/Рекомендація	Враховано / частково враховано / не враховано	Примітка
Шаповал О. С., виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»	Приділити більше уваги опануванню принципів безпеки в базах даних. Акцентувати увагу на вивченні хмарних технологій і DevOps.	Враховано.	До перліку вибірових освітніх компонентів додано дисципліни: «Безпека в DEVOPS», «Бази даних з SQL і Python».
Гарант ОПП, завідувач кафедри, д.т.н., професор Євсєєв С.П. Члени робочої групи ОПП	Освітньо-професійну програму привести у відповідність до вимог Стандарту вищої освіти за спеціальністю 125 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 24.10.2024р. № 1547.	Враховано.	Освітньо-професійна програма відповідає вимогам Стандарту вищої освіти за спеціальністю 125 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 24.10.2024р. № 1547.
Гарант ОПП, завідувач кафедри, д.т.н., професор Євсєєв С.П. Члени робочої групи ОПП	Зміна шифру спеціальності та галузі знань (згідно з постановою Кабінету Міністрів України від 30 серпня 2024 р. No 1021).	Враховано.	Зміни внесено.
Волощук О. Б., к. т. н., керівник освітніх програм ТОВ “Distributed Lab”	Позитивний відгук. Без зауважень.	-	-
Опірський І. Р., доктор технічних наук, професор,	Позитивний відгук. Без зауважень.	-	-

завідувач кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»			
Ковтун В. Ю., кандидат технічних наук, доцент, директор ТОВ «Сайфер»	Позитивний відгук. Без зауважень.	-	-
Головашич С. О., кандидат технічних наук, доцент директор ТОВ «Мікрокрипт Текнолоджіс»	Позитивний відгук. Без зауважень.	-	-

Завідувач кафедри кібербезпеки _____ Сергій ЄВСЕЄВ

Гарант освітньої програми _____ Сергій ЄВСЕЄВ

9. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ/РЕКОМЕНДАЦІЙ ЗА РЕЗУЛЬТАТАМИ АКРЕДИТАЦІЙНОЇ ЕКСПЕРТИЗИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/до вгостроковий/не доцільно враховувати)	Заходи, що спрямовані на врахування рекомендацій/Обґрунтування щодо недоцільності впровадження рекомендації	Терміни впровадження заходів/відповідальні особи
Загальні рекомендації Експертної групи та Галузевої експертної ради (по кафедрі, галузі, інституту, університету)			
Переглянути в наступній редакції ОПП перелік затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010.	Довгостроковий	Оновлення у ОПП переліку затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП.
Посилити поінформованість студентів щодо внутрішніх процедур організації освітнього процесу. Рекомендовано переглянути та оновити літературу в силабусах освітніх компонентів.	Довгостроковий	Проведення опитувань серед студентів щодо внутрішніх процедур організації освітнього процесу. Перегляд та оновлення літератури в силабусах освітніх компонентів. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: завідувач кафедри КБ, викладачі кафедри.
Використання кіберполігону для ознайомлення здобувачів з його можливостями	Довгостроковий	Залучення фахівців з кібербезпеки та захисту інформації регулярно брати участь у навчанні та	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП,

		тренуванні на кіберполігоні. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	завідувач кафедри КБ.
Забезпечувати постійне оновлення інформації щодо всіх аспектів провадження ОПП на сайті кафедри.	Довгостроковий	Інформації щодо всіх аспектів провадження ОПП постійно оновлюється на сайті кафедри. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП.

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних технологій _____ Михайло ГОДЛЕВСЬКИЙ

Гарант освітньої програми _____ Сергій ЄВСЕЄВ